Remarks/Arguments

STATUS OF CLAIMS

Claims 1-5, 8-10 and 12-17 are pending.

Claims 1-5, 8-10 and 12-17 stand rejected.

Claims 7, 13 and 15 are amended, without prejudice or disclaimer.

Rejection of Claims 7, 13 and 15 under 35 USC 112, second paragraph

Claims 7, 13, and 15 stand rejected under 35 USC, second paragraph, as being indefinite, on the grounds that those claims recite the limitation "decrypting an encrypted part of the content" and "decrypting the downloaded content." The Examiner states that the independent claims do not disclose that content is encrypted.

Claims 7, 13 and 15 have each been amended, without prejudice or disclaimer, to recite that a part of the content, or the content, are encrypted, consistent with the recited limitations. Disclosure support for these amendments may be found, for example, in the specification at page 4, lines 15-17.

For these reasons, it is respectfully submitted that this rejection has been overcome.

Rejection of Claims 1-5, 7-10 and 12-17 under 35 USC 102(e) as being anticipated by Chan et al. (U.S. Patent No. 6,233,683).

Claims 1-5, 7-10 and 12-17 stand rejected under 35 U.S.C. 102(e) as being anticipated by Chan et al. (U.S. Patent No. 6,233,683). Applicants submit that for the reasons discussed below Chan fails to disclose each and every limitation of independent claims 1 and 10, and as such, these claims, and the claims that depend therefrom, are not anticipated by Chan.

In summary, as to claim 1, Chan does not disclose steps of verifying that an entitlement in the card is correct for receiving and using content. Instead, Chan discloses verification of a signature that verifies the source of content.

Claim 1 recites:

1. A method for using an integrated circuit card to facilitate downloading and use of content from a server to a terminal,

receiving content broadcast from a server;

verifying that an entitlement contained in the integrated circuit card is correct for receiving the content;

receiving the reusable content from the server via the terminal in response to the verification;

storing the reusable content in response to the verification, and

verifying that the entitlement is correct for reuse when reuse of the content is attempted.

Applicants submit that Chan fails to disclose or suggest at least the above-emphasized limitations of amended claim 1.

Chan discloses a system, implemented in software on a smart card, which enables the downloading *to the smart card* of new applications and data for use by applications (col. 5, lines 25-28). By contrast, the method of claim 1 is a method for using a smart card in downloading *to a terminal.* Chan's system discloses verification of signatures to verify the *source* of content; the method of claim 1 discloses entitlement information used to verify a right to receive and use the content. For at least these reasons, claim 1 is not anticipated by Chan.

The system of Chan may be understood by reference to Figs. 3A and 3B and accompanying text. Chan discloses, in Figs. 3A and 3B, software components of a smart card (col. 5, lines 16-18). The software components in the example in Fig. 3A include an operating system 300, a card API 304, applications 305A-305C, a card domain 308 and open platform API 306. Card domain 308 can perform functions such as installing an application on the smart card (col. 5, lines 56-57). In Fig. 3B of Chan, there is an additional software component, namely security domain 310. The security domain works with applications of the card domain to provide security related functions to the card domain (abstract, col. 6, lines 62-66). In particular, the security domain manages signing and decrypting keys and provides cryptographic services using those keys (col. 7, lines 51-65). The security domain can be loaded onto the smart card before or after the smart card is issued (col. 8, lines 28-54). Once loaded, the security domain provides the security functions mentioned above.

Among the information that may be downloaded to the card in accordance with the disclosure of Chan is confidential personalization information.

Confidential personalization information, as explained in Chan at col. 2, lines 47-51, may include a maximum value of the card, a PIN, the currency in which the card is valid, the expiration date of the card, and cryptographic keys for the card. The Examiner takes the position, on page 4 of the Office Action, that such confidential personalization information constitutes an entitlement as recited in claim 1. In particular, the Examiner states: "Chan teaches the confidential personalization (entitlement) information contained in the card is verified and the application (content) is installed."

In response, it is respectfully submitted that one of ordinary skill in the art would not interpret the term "entitlement" as reading on "confidential personalization information" as disclosed in Chan. First, as described in Applicant's specification, for example at page 4, lines 11-17, entitlements are typically known as "entitlement management messages" (EMM) and are associated with particular downloadable software applications or other reusable content. Each entitlement represents a future right to download a software application or other reusable content, or a right to decrypt and/or use previously encrypted software or reusable content." An entitlement, as used in claim 1, will be understood by one of ordinary skill in the art as identifying a right to receive, decrypt or use content. In contrast, the "personalization information" of Chan does not represent such rights. Confidential personalization information, as noted above, relates to attributes of the card, such as maximum storage. Entitlements define a relationship to identified software applications or other content.

Applicant acknowledges, as noted by the Examiner on page 4 of the Office action, that the subject matter of the independent claims is broadly recited. However, the breadth of meaning that the Examiner may attribute to claim language is limited by the broadest reasonable interpretation that would be ascribed to the language by one of ordinary skill in the art, interpreting the claims in light of the specification. One of ordinary skill in the art would not reasonably interpret the term "entitlement" as used in claim 1 to cover the "personalization information" of Chan. As noted above, the term "entitlement" is referenced in Applicant's specification as "entitlement management message." An entitlement management message provides information as to a right to receive or use particular content. In view of the ordinary meaning of "entitlement," and the

foregoing reference to the term "entitlement" in the specification, one of ordinary skill in the art would not reasonably interpret "entitlement management message" to cover attributes of a card, such as the confidential personalization information described in Chan.

The foregoing represents sufficient grounds for withdrawal of the rejection of claim 1 over Chan. The foregoing notwithstanding, the rejection should be withdrawn for the following independent reason. The Examiner states, also on page 4 of the Office Action, that the personalization information is verified and the application is installed. In particular, the Examiner states: "the confidential personalization (entitlement) information contained in the card is verified and the application (content) is installed." The Examiner apparently takes the position that Chan teaches the steps of "verifying that an entitlement contained in the integrated circuit card is correct for receiving the content" and "receiving the reusable content from the server via the terminal in response to the verification." However, Chan does not disclose or suggest verification of personalization information. The personalization information may be signed, in which case the security domain's signature check is invoked (col. 12, lines 47-51). However, a signature check verifies that the personalization information was provided by the proper *source*, not that the personalization information "is correct for receiving the content" as recited in claim 1. In other words, the claimed step of "verifying that an entitlement contained in the integrated circuit card is correct for receiving the content" requires that the *substance* of the entitlement communicate that the card have a right to receive the content. Chan's signature check, by contrast, looks only to the *source* of the personalization information, and not to the substance of the personalization information. This represents further independently sufficient grounds for withdrawal of the rejection over Chan.

In addition to the independently sufficient grounds stated above, there is yet further independent grounds for withdrawal of the rejection. The Examiner further states, on page 4 of the Office Action, that "Chan teaches if the application is already loaded (reuse of content), then the loaded application invokes the cryptographic service to decrypt the associated application." The Examiner states that "at each instance the verification that the content is correct of reuse is rechecked." However, Chan does *not* teach *verification* of a right to reuse the

content. Instead, Chan merely teaches *decrypting* the content. In particular, if the personalization information is encrypted, the decryption service of the security domain of the card is invoked (col. 12, lines 47-51). The decryption of content does *not* meet the limitation: "verifying that the entitlement is correct for reuse when reuse of the content is attempted." This verifying step requires checking the substance of the entitlement to determine whether there is a right to reuse the particular content. Decryption of encrypted content, as disclosed in Chan, does not relate to determining whether there is a right to use such content. This represents further independently sufficient grounds for withdrawal of the rejection over Chan.

The portions of Chan cited by the Office Action fail to disclose or suggest the limitations of claim 1 discussed above. Col. 3, lines 38-45 discuss providing first and second applications to a smart card, wherein the cryptographic service of the first application is used to load the second application. Col. 12, lines 14-53 describe the method shown in Figs. 12A and 12B, in which a trusted agent is used in generating and sending cryptographic keys to the smart card for verification and processing of the new application. Again, in this scenario, the security domain is invoked to verify the signature associated with the application and provide cryptographic services (col. 12, lines 41-44). Clearly, none of the cited portions of Chan disclose or suggest verifying an entitlement contained in the smart card. As no verification is taught in Chan, Chan does not teach or suggest the steps of: "... receiving the reusable content from the server via the terminal in response to the verification;" or "storing the reusable content in response to the verification" as recited in claim 1.

In view of the foregoing, the Applicant has explicitly identified specific claim limitations which are neither taught nor suggested in Chan or the other prior art of record. For at least the foregoing reasons, claim 1 is allowable over the prior art of record.

Claims 2-5 and 7-9 depend from claim 1 and are allowable at least by virtue of their dependence from an allowable base claim.

Independent Claim 10 reads as follows:

> 10. A system for securely downloading, and using content from a server, the system comprising:
>
> a terminal, communicatively coupled to the server, having a processor for processing the download of the content from the server, a memory for receiving the downloaded content and an integrated circuit card interface circuit;
>
> wherein an integrated circuit card, coupled to said interface circuit, provides an entitlement message enabling said terminal to download the content from a server, the integrated circuit card containing an entitlement database for storing a plurality of entitlements;
>
> and wherein the integrated circuit card provides an entitlement message enabling said terminal to reuse the content from a server.

Claim 10, similarly to claim 1, recites providing an entitlement message, and is allowable at least for the reasons that claim 1 is allowable.

Moreover, claim 10 is allowable for at least the additional reason that Chan nowhere teaches or suggests the limitations "an integrated circuit card ... provides an entitlement message enabling said terminal to download the content from a server," and "the integrated circuit card provides an entitlement message enabling said terminal to reuse the content from a server." In Chan, applications are added *to the card*, not a distinct terminal. Similarly, in Chan, applications are executed on the card, not by a separate terminal. The Examiner identifies these limitations as being taught at col. 3, lines 38-45 and col. 12, lines 14-53. As noted above, col. 3, lines 38-45 discuss providing first and second applications to a smart card, wherein the cryptographic service of the first application running on the smart card is used to load the second application. Col. 12, lines 14-53 describe the method shown in Figs. 12A and 12B, in which a trusted agent is used in generating and sending cryptographic keys to the smart card for verification and processing of the new application loaded on the smart card. Neither of these portions of Chan has any hint or suggestion of the above-quoted limitations of claim 10.

For at least the foregoing reasons, claim 10 is allowable over the prior art of record.

Claims 12-13 depend from claim 10 and are allowable at least by virtue of their dependence on an allowable base claim.

Independent claim 14 reads as follows:

> 14. A system for downloading and reusing content from a server, comprising:
>
> a receiver communicatively coupled to a server and adapted to receive reusable content from the server;
>
> an integrated card interface adapted to receive an integrated circuit card;
>
> a memory;
>
> a processor coupled to the receiver, the integrated card interface, and the memory, the processor enabling reusable content from the server to be received and stored in the memory in response to entitlement information received via the integrated card interface, the processor enabling reuse of the reusable content stored in memory in response to entitlement information received via the integrated card interface.

Independent claim 14, like claim 1, recites entitlement information. For the reasons discussed above in connection with claim 1, Chan does not disclose or suggest entitlement information as recited in claim 14.

In addition, claim 14 recites a system having a processor which enables reusable content from a server to be downloaded in response to entitlement information received via a card interface, and which enables the content to be reused in response to entitlement information received via the card interface. Chan does not teach a system having a processor which enables downloading and use of content in response to information of any kind received via a card interface. Rather, Chan relates to loading of applications on a smart card, *not on a system distinct from the smart card*. Thus, Chan does not teach or suggest at least the following limitations of claim 14:

> a processor coupled to the receiver, the integrated card interface, and the memory, the processor enabling reusable content from the server to be received and stored in the memory in response to entitlement information received via the integrated card interface, the processor enabling reuse of the reusable content stored in memory in response to entitlement information received via the integrated card interface.

For at least the foregoing reasons, claim 14 is allowable.

Claims 15-18 depend from claim 14, and are allowable at least by virtue of their dependency from an allowable base claim.

CONCLUSION

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

Weaver, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 8/16/06